Cybersecurity firm Qualys is the latest victim of Accellion hacks

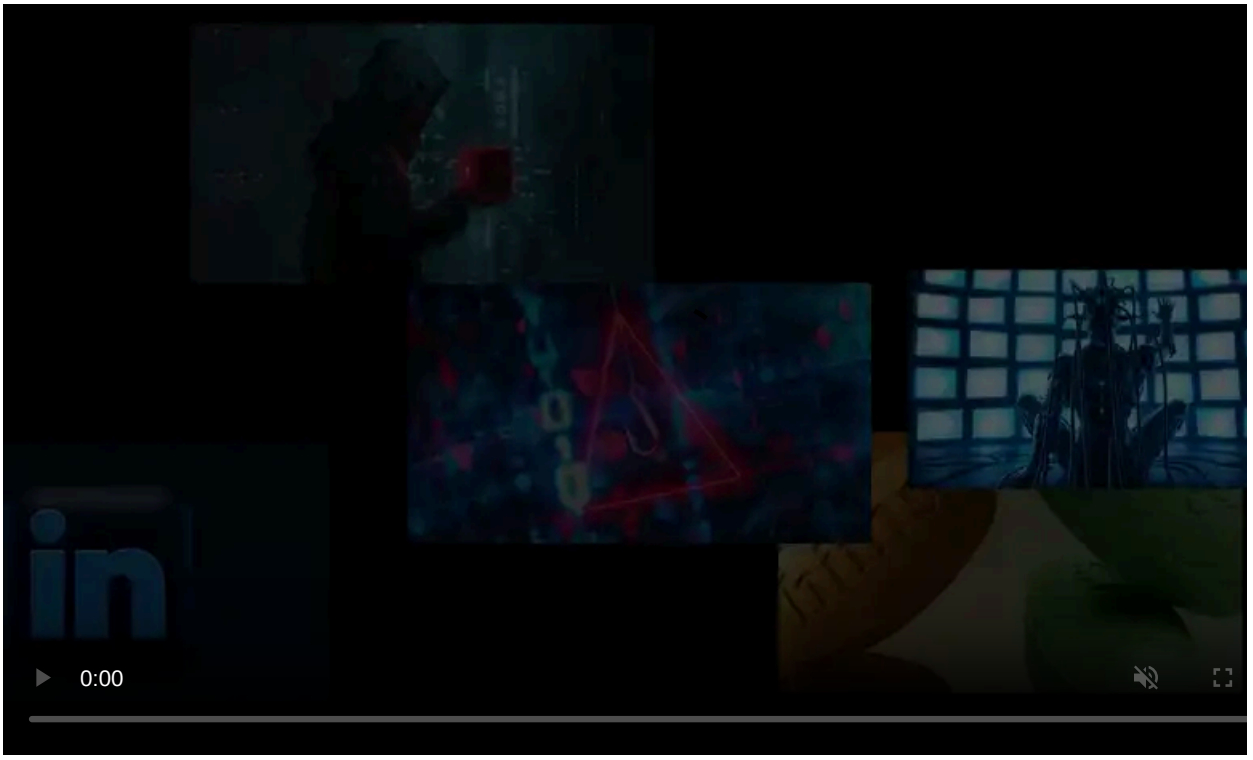
By Lawrence Abrams

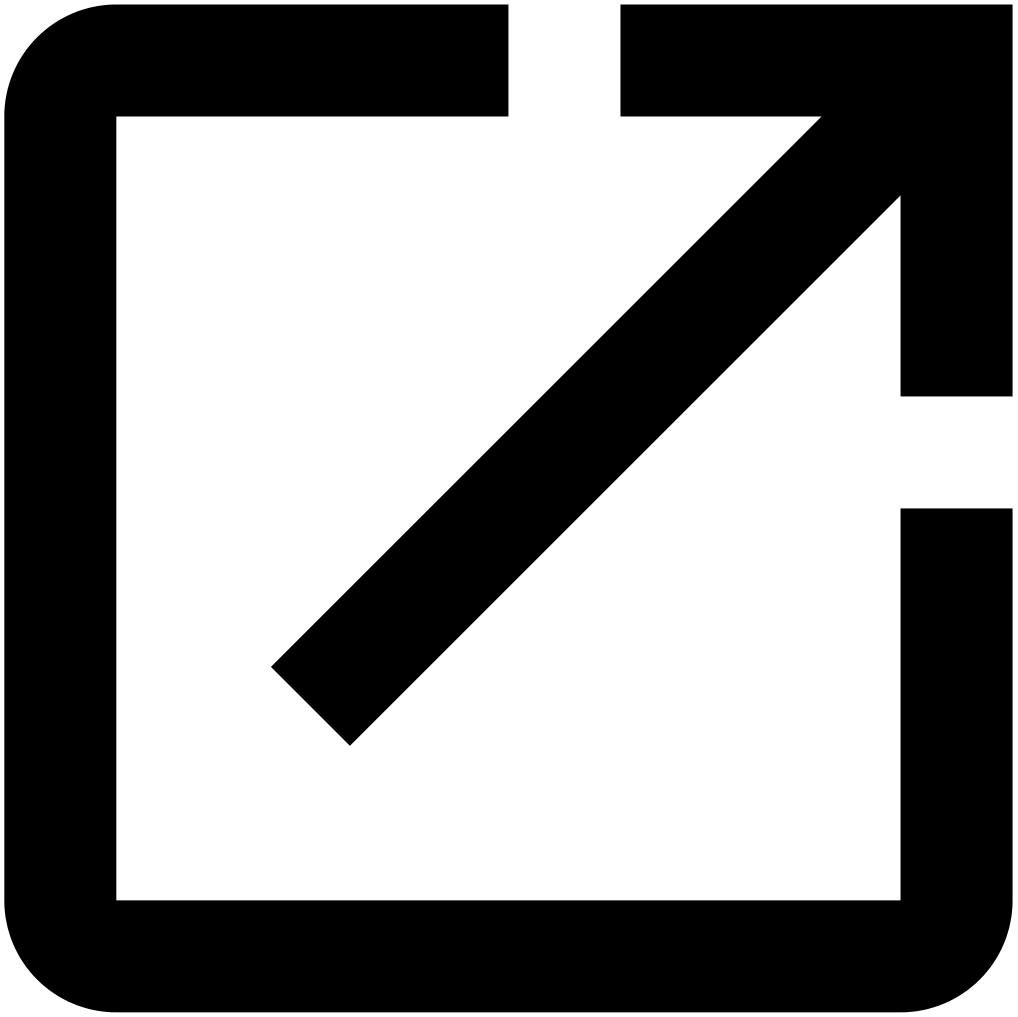
Published: 2021-03-03 · Archived: 2026-04-05 16:04:00 UTC

Cybersecurity firm Qualys is likely the latest victim to have suffered a data breach after a zero-day vulnerability in their Accellion FTA server was exploited to steal hosted files.

In December, a wave of attacks targeted the Accellion FTA file-sharing application using a zero-day vulnerability that allowed attackers to steal files stored on the server.

Since then, the Clop ransomware has been extorting these victims by posting the stolen data on their ransomware data leak site.


0:00



As Accellion FTA devices are standalone servers designed to be outside the security perimeter of a network and accessible to the public, there have been no reported attacks on these devices leading to internal systems compromise.

Before today, the known victims extorted by Clop include Transport for NSW, Singtel, Bombadier, geo-data specialist Fugro, law firm Jones Day, science and technology company Danaher, and technical services company ABS Group.

Qualys the latest victim to be extorted

Yesterday, the Clop ransomware gang posted screenshots of files allegedly belonging to the cybersecurity firm Qualys. The leaked data includes purchase orders, invoices, tax documents, and scan reports.

As reported by Valery Marchive of LegMagIT and confirmed by BleepingComputer, Qualys had an Accellion FTA device located on their network.

The Accellion FTA device was located at fts-na.qualys.com, and the IP address used by the server is assigned to Qualys. Qualys has since decommissioned the FTA device, with Shodan showing it was last active on February 18th, 2021.

It is unknown if Clop sent ransom notes to Qualys regarding the attack, but other victims have received them in the past, according to a report by Mandiant.

> Hello!
>
> Your network has been hacked, a lot of valuable data stolen. <description of stolen data, including the total size of the compressed files> We are the CLOP ransomware team, you can google news and articles about us. We have a website where we publish news and stolen files from companies that have refused to cooperate. Here is his address http://[redacted].onion/ - use TOR browser or http://[redacted].onion.dog/ - mirror. We are visited by 20-30 thousand journalists, IT experts, hackers and competitors every day. We suggest that you contact us via chat within 24 hours to discuss the current situation. <victim-specific negotiation URL> - use TOR browser We don't want to hurt, our goal is money. We are also ready to provide any evidence of the presence of files with us.

Ransom note sent to Accellion FTA victims

It is still unclear if the Clop ransomware gang performed the attacks on Accellion FTA devices or is partnering with another group to share the files and extort victims publicly.

Clop has in the past sent emails to journalists, including BleepingComputer, about new Accellion FTA victims posted to their site.

BleepingComputer has contacted Qualys before publication and are awaiting an official statement.

Qualys confirms Accellion FTA breach

In a statement issued tonight, Qualys has confirmed that their Accellion FTA server was breached in December 2020 and affected a limited amount of customers.

As the server was deployed in their DMZ, which is segregated from their internal network, Qualys' product environment was not compromised.

"New information has come out today related to a previously identified zero-day exploit in a third-party solution, Accellion FTA, that Qualys deployed to transfer information as part of our customer support system."

"Qualys has confirmed that there is no impact on the Qualys production environments, codebase or customer data hosted on the Qualys Cloud Platform. All Qualys platforms continue to be fully functional and at no time was there any operational impact."

"Qualys had deployed the Accellion FTA server in a segregated DMZ environment, completely separate from systems that host and support Qualys products to transfer information as part of our customer support system," Qualys disclosed in a security incident notice today.

Qualys states that they have shut down the affected Accellion FTA servers and switched to alternative applications for support-related file transfers.

At this time, Qualys is still investigating the breach and has hired Mandiant to assist them.

Source: https://www.bleepingcomputer.com/news/security/cybersecurity-firm-qualys-is-the-latest-victim-of-accellion-hacks/